UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

EPIC SYSTEMS CORPORATION, a Wisconsin Corporation,

Plaintiff,

Case No. 14-CV-748

v.

TATA CONSULTANCY SERVICES LIMITED, an Indian Corporation; and TATA AMERICA INTERNATIONAL CORPORATION (dba TCS AMERICA), a New York Corporation,

Defendants.

[PROPOSED] PERMANENT INJUNCTION

Defendants Tata Consultancy Services Limited and Tata America International Corporation have been found liable for the following: (1) trafficking of passwords and obtaining information from a protected computer without authorization in violation of the Computer Fraud and Abuse Act; (2) willfully and knowingly accessing Epic's UserWeb without authorization and sharing of passwords in violation of the Wisconsin Computer Crimes Act; (3) fraudulent misrepresentation; (4) misappropriation of trade secrets; (5) unfair competition; (6) unjust enrichment; (7) deprivation of property; and (8) breach of the parties' Standard Consultant Agreement by (i) failing to limit access to Epic's UserWeb and to materials obtained from UserWeb to employees who needed access in order to perform testing services for Kaiser, (ii) using Epic's confidential information for purposes other than implementing Epic's software on Kaiser's behalf, (iii) permitting TCS employees with access to Epic's confidential information to consult with other TCS employees concerning the development or enhancement of TCS's Med Mantra software, (iv) failing to maintain Epic's confidential information in confidence, (v)

failing to store copies of Epic's confidential information in a safe place, and (vi) failing to provide prompt written notice of TCS employees' unauthorized access to Epic's UserWeb. Dkt. No. 538 at 65; Dkt. No. 855.

The Computer Fraud and Abuse Act (18 U.S.C. § 1030), Wisconsin's Uniform Trade Secrets Act (Wis. Stat. § 134.90(3)(a)(1)) and Wisconsin's Computer Crimes Act (Wis. Stat. § 943.70) provide for injunctive relief to be granted where a violation of these statutes is established. TCS also acknowledged that its breach of the parties Standard Consulting Agreement may result in irreparable harm to Epic. *See* Trial Ex. 3 at 8(a).

Based on the record in this case, the Court hereby enters the following Permanent Injunction under Federal Rule of Civil Procedure 65 upon finding good cause therefor:

1. For purposes of the Permanent Injunction, the following terms apply:
    a. "Epic" shall mean plaintiff Epic Systems Corporation.
    b. "TCS" shall mean Tata Consultancy Services Limited and Tata America International Corporation.
    c. "Trade Secret or Confidential Information" shall mean and include the information contained in the 1,687 unique documents TCS downloaded from Epic's UserWeb, Program Property as that term is defined in the Standard Consulting Agreement (Trial Ex. 3) and any other Epic confidential or trade secret information acquired by TCS in performing its testing services for Kaiser Permanente.
2. TCS and their respective affiliates, successors, officers, agents, servants, employees, and attorneys and any and all other persons who are in active concert or participation with any of them (all collectively referred to as "Enjoined Parties"), are permanently enjoined, anywhere in the world, from the following:
    a. using any Epic Trade Secret or Confidential Information for any reason, including but not limited in the design, development, enhancement, or marketing of any TCS software providing solutions in the areas of electronic

health records, electronic medical records, and hospital management systems, or any other healthcare software solutions, including but not limited to Med Mantra (as most broadly defined, including but not limited to, TCS-HIS, Med Mantra in use at Apollo Hospitals in India, British American Hospital in Mauritius, Tata Cancer Hospital in India, Tata Cancer Institute in India, and Med Mantra modules in development at DaVita Healthcare Partners, Inc. and Quest Diagnostics, Inc.) (collectively, "TCS EHR Products");

b. possessing or retaining any Epic Trade Secret or Confidential Information in any form, including on any servers or other electronic computer systems of TCS or any other electronic or hard-copy media at TCS;

c. accessing or attempting to access any non-public Epic servers or systems, including Epic' internet portal known as UserWeb; and

d. permitting any TCS employee or consultant or agent who had access, or may have had access, to any Epic Trade Secret or Confidential Information to work on, or assist in, directly or indirectly, the design, development, enhancement, or marketing of any TCS EHR Products.

3. For at least the next four years, and for as long thereafter as the Court deems appropriate, TCS shall not resist, hamper, delay, or otherwise interfere with the activities of an ombudsman or monitor to be jointly selected by TCS and Epic (or the Court if the parties do not agree), and promptly paid by TCS, who shall have unfettered access at any time, to monitor TCS's development and implementation of any TCS EHR Products to ensure that TCS does not improperly use any of Epic's Trade Secrets or Confidential Information, as described below. In particular, TCS shall permit the ombudsman or monitor to:

a. Confirm that TCS employees, consultants, and agents do not have access to Epic's internet portal known as UserWeb or to any of Epic's Trade Secret or Confidential Information.

b. Confirm that TCS does not possess or retain any Epic Trade Secret or Confidential Information on any of its servers, shared drives, shared domains, or other places of electronic information storage.

c. Talk with any TCS employee who might be able to assist the ombudsman or monitor in determining whether Epic Trade Secret or Confidential Information was or is being used in the design, development, enhancement, or marketing of any TCS EHR Products. TCS shall provide the ombudsman or monitor with unfettered access to these TCS employees.

d. Examine, evaluate, and analyze TCS's electronic information, including TCS's proxy logs, domain logs, active directory logs, software, servers, shared drives, and shared domains, to determine whether any Epic Trade Secret or Confidential Information was or is being used or is intended to be used in the design, development, enhancement, or marketing of any TCS EHR Products. TCS shall provide the ombudsman or monitor with unfettered access to this electronic information.

4. Epic shall have the ability to confidentially provide the investigative firm with the type of information Epic's deems necessary to monitor TCS's development and implementation of any TCS EHR Product to ensure that TCS does not improperly use any of Epic's Trade Secret or Confidential Information.

5. Within 20 court days of the effective date of this Permanent Injunction, TCS shall file and serve a report in writing and under oath setting forth in detail the manner and form with which TCS has complied with the Permanent Injunction.
6. Violation of Permanent Injunction shall be subject to all applicable penalties, including contempt of Court.
7. This Court shall retain continuing jurisdiction over Epic, TCS and the Enjoined Parties and the action for the purpose of enforcing the Permanent Injunction.

IT IS SO ORDERED this _____ day of _____, 2016.

_____

Chief Judge for the Western District of Wisconsin